HOUSE BILL REPORT
HB 1031

As Reported by House Committee On:
Technology, Energy & Communications

Title: An act relating to electronic communication devices.

Brief Description: Changing provisions concerning electronic devices.

Sponsors: Representatives Morris, Hudgins, Moeller, Linville, B. Sullivan and Chase.

Brief History:
Committee Activity:
Technology, Energy & Communications: 1/10/07, 2/23/07 [DPS].

Brief Summary of Substitute Bill

- Requires that a person selling or issuing an electronic communication device that has not been disabled, deactivated, or removed at the point of sale or issuance, provide notice to the consumer and label the device.
- Requires that a person selling or issuing an electronic communication device must use industry accepted best standards to secure the device.
- Prohibits a person from remotely scanning or reading an electronic communication device to identify a consumer without obtaining consent from the consumer.
- Creates civil penalties.

HOUSE COMMITTEE ON TECHNOLOGY, ENERGY & COMMUNICATIONS

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Morris, Chair; McCoy, Vice Chair; Crouse, Ranking Minority Member; McCune, Assistant Ranking Minority Member; Eddy, Hudgins, Hurst, Takko and VanDeWege.

Minority Report: Without recommendation. Signed by 2 members: Representatives Ericksen and Hankins.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

Staff: Kara Durbin (786-7133).

Background:

Overview of Federal Privacy Laws
Federal law contains a number of protections with respect to individual privacy.

The federal Privacy Act of 1974 protects unauthorized disclosure of certain federal government records pertaining to individuals. It also gives individuals the right to review records about themselves, to find out if these records have been disclosed, and to request corrections or amendments of these records, unless the records are legally exempt. The federal Privacy Act applies to the information gathering practices of the federal government, but does not apply to state or local governments, or to the private sector.

In addition to the federal Privacy Act, there are other federal laws that limit how personal information can be disclosed. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices. Generally, if a financial institution shares a consumer's information, it must give the consumer the ability to "opt-out" and withhold their information from being shared. The Fair Credit Reporting Act (FCRA) generally requires that credit reporting agencies follow reasonable procedures to protect the confidentiality, accuracy, and relevance of credit information. To accomplish this, the FCRA establishes a framework of fair information practices for personal information maintained by credit reporting agencies that includes the right to access and correct data, data security, limitations on use, requirements for data destruction, notice, consent, and accountability. In addition, the Health Insurance Portability and Accountability Act (HIPAA) limits the sharing of individual health and personal information.

Washington's Privacy Act
The Washington Privacy Act, chapter 9.73 RCW, restricts the interception or recording of private communications or conversations. As a general rule, it is unlawful for any person to intercept or record a private communication or conversation without first obtaining the consent of all parties participating in the communication or conversation. There are some limited exceptions to this general rule that allow the communication or conversation to be intercepted and recorded when only one party consents, or allow it to be intercepted pursuant to a court order.

Certain persons and activities are exempt from the state Privacy Act, including common carriers in connection with services provided pursuant to its tariffs on file with the Washington Utilities and Transportation Commission and emergency 911 service.

In addition to the Washington Privacy Act, Washington law contains a number of provisions with respect to invasions of privacy, including provisions related to identity theft, computer theft, stalking, and "skimming" crimes, which refers to when an identification or payment card is copied for illegal purposes.

Radio Frequency Identification

Radio Frequency Identification (RFID) is a tagging and tracking technology that uses tiny electronic devices equipped with antennae, which can transmit identifying information to a remote reader. The information gathered by the reader can be stored or matched to an existing record in a database. Most RFID tags can be read at a distance and often without the knowledge of the person who carries the item containing the RFID tag.

There are no federal or state laws that specifically prohibit or restrict the use of RFID.

Summary of Substitute Bill:

Definition of Electronic Communication Device
An electronic communication device is defined as any device that passively or actively uses RFID technology in the 902 - 928 MHz frequency range or the 2.4 GHz frequency authorized by the Federal Communications Commission (FCC), or any subsequent frequency range authorized by the FCC for RFID technology as may be provided by the FCC by rule.

Definition of Person
Person is defined as an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture government, government subdivision, agency or instrumentality, public corporation, or any other legal or commercial entity.

Labeling
If a person sells or issues an electronic communication device that has not been disabled, deactivated, or removed at the point of sale or issuance, the device must be clearly and conspicuously labeled. The label must contain a universally accepted symbol for RFID technology and be affixed to the electronic communication device or its packaging.

Notice
If a person sells or issues an electronic communication device that has not been disabled, deactivated, or removed at the point of sale or issuance, the person must either: (1) post signs providing information to the consumer about the existence of a universally accepted symbol for identifying the electronic communication device; or (2) distribute information to the consumer that explains the meaning of the universally accepted symbol.

The signs must be posted in prominent areas near the point of sale or issuance, and the signs and lettering must be clearly visible to consumers.

The signs must display the following information:

- an explanation of the universally accepted symbol, which indicates that the person is selling or issuing an electronic communication device;
- an explanation of how an electronic communication device may send, gather, or transmit information about the consumer, which could be read by an unauthorized third party; and
- instructions on whether it is technically feasible to deactivate or remove the electronic communication device, and, if technically feasible, instructions must be provided on the

specific location of the electronic communication device and how the consumer may seek deactivation or removal of the device.

Transmission of Personal Information
If the electronic communication device transmits personal information about a consumer, a person must, prior to sale or issuance of the device, notify the consumer and secure a consent acknowledgment or manifest assent from the consumer.

Removal or Deactivation
If the consumer consents to the use of an electronic communication device, either through a consent acknowledgment or manifest assent, but later requests removal or deactivation of the electronic communication device, the consumer may be held responsible for any costs associated with deactivation or removal.

Once an electronic communication device has been deactivated, it must not be reactivated without the manifest assent of the consumer identified with the electronic communication device.

Requiring Use
A consumer shall not be coerced into keeping an electronic communication device active on the item in order for the consumer to be able to exchange, return, repair, or service the item.

Security Measures
A person who sells or issues an electronic communication device that has not been disabled, deactivated, or removed at the point of sale or issuance must use industry accepted best standards to secure the electronic communication device. A person who retains personal information gathered through an electronic communication device must implement adequate security measures. The security measures should be consistent with industry standards that are commensurate with the amount and sensitivity of the information being stored on the system.

Unauthorized Scanning
A person may not use an electronic communication device to remotely scan or read, or attempt to scan or read, an electronic communication device to identify a consumer without obtaining a consent acknowledgment or manifest assent from the consumer.

This prohibition does not apply to the following situations:

- scanning or reading an electronic communication device, or using information gathered through an electronic communication device, in order to comply with federal law or regulations, or state law;
- scanning or reading an electronic communication device, or using information gathered through an electronic communication device, in order to comply with properly authorized civil, criminal, administrative, or regulatory investigation, subpoena, or summons by federal, state, or local authorities;
- scanning or reading an electronic communication device, or using information gathered through an electronic communication device, in order to respond to judicial process or

government regulatory authorities having jurisdiction over the person for examination, compliance, or other purposes as authorized by law.

Penalties
The Attorney General may bring an action against a person who violates this bill to enjoin further violations and seek either actual damages or $10,000 for each separate violation. Multiple violations resulting from any single action or conduct shall constitute a violation. If the defendant has engaged in a pattern or practice of violating this bill, the court may award damages of up to three times the original amount and may award costs and reasonable attorneys' fees to a prevailing party.

Exemption
This bill does not apply to the resale of an electronic communication device by a consumer.

The bill contains a severability clause.

Substitute Bill Compared to Original Bill:

The substitute bill removes some of the consumer privacy rights outlined in the original bill. The substitute bill narrows the definition of an electronic communication device to reflect a device that passively or actively uses radio frequency identification (RFID) technology in certain frequency ranges authorized by the Federal Communications Commission. The substitute bill removes a definition of "item" and "unique identifier number." The substitute bill adds a definition of "identify,""radio frequency identification," and "universally accepted symbol."

The substitute bill removes the consumer's ability to request any stored personal information pertaining to them. The substitute bill removes the prohibition on combining or linking a consumer's personal information with information gathered from an electronic communication device. The substitute bill removes the provisions related to disclosure of information gathered by an electronic communication device. The substitute bill removes the private right of action and adds a provision allowing the Attorney General to bring a civil action to enforce the bill. The substitute bill removes the criminal penalties. The substitute bill adds a severability clause.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Substitute Bill: The bill takes effect 90 days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony:

Testimony on proposed substitute bill heard January 10, 2007

(In support) I am really pleased to see this bill coming forward. This bill attempts to strike a good balance between the needs for privacy and the needs for businesses to transact electronically. This is the right timing for this. We need to protect people's privacy. Privacy policies are critical, but consumers need to know that they retain their privacy and that they're not being tracked through the merchandise they purchase. I strongly support this bill. I feel the notice and labeling provisions are very important.

(In support with concerns) It is important that we get ahead of this technology and not wait for the violations to start occurring. We have worked with other sponsors on legislation with respect to RFID and will continue to support such efforts. We hope these protections can be put in place.

(With concerns) This would impact our automatic meter readers.

(Opposed) We are committed to protecting our customer's confidential information. We are concerned that there may be some unintended consequences with this bill. We are already heavily regulated regarding customer proprietary network information. This is unnecessarily burdensome. This could require complex changes to our business practices, yet we're not sure whether there's a problem with the capture of data from wireless phones. This bill should focus on nefarious use of customer information. We have strong privacy policies already in place. We have significant concerns with this bill. We believe RFID will be a part of our financial future. These RFID devices will continue to be embedded in debit and credit cards. These devices are convenient and secure. We believe this bill could cause great havoc on financial transactions. This would significantly inhibit the ability for debit and credit card transactions to occur. We believe RFID has some very good potential uses. Security issues are better addressed at the design level. This bill is moving in the right direction but it raises too many questions. Government use of RFID is much more concerning than the private sector. Supply chain visibility is a great use of RFID as well as anti-counterfeit purposes. We don't want to stifle this industry prematurely. We support state consumer protections, but don't feel this is the appropriate approach. We'd prefer to see bans on unauthorized use of the technology.

Testimony on proposed substitute heard on February 16, 2007

(In support) I wanted to get comments in the record based on the new draft. I have removed the watermarking and disclosure provisions of the bill. I want to get key components into code and then take a closer look at other issues over the interim. I have held five workgroup meetings during session, and I held meetings before session. There has been a varying level of participation in this bill from the stakeholders. I think this is a critical issue for us to understand and I think the bill has come a long way.

We applaud you for bringing this bill forward to address the privacy risks associated with these types of technologies. We encourage you to incorporate new technologies and to pursue additional enforcement mechanisms. Victims are being found through readily available data sources. Unique identifiers can still become identifiable. We would like to see this bill limit the collection of personal data. We strongly urge you to see this effort through. It is

interesting that there is so much opposition to this straightforward bill. It is providing for labeling and notice to consumers. The technology is great, but we must protect the privacy of our consumers. Consumers should have notice of the presence of the readers. Tag numbers can be collected, collated and used to identify consumers. These tag numbers should be included in the bill.

(In support with concerns) This is just a starting point. Adding RFID to items that we carry around allow those items to become associated with our person. We believe we should have control over who accesses that information. This is extremely important. It is important for the state to put some parameters around this technology. We appreciate the notice, but would like notice to be given whether the device transmits personal information or not. We appreciate the labeling and deactivation provisions. We would like to see the private cause of action and the Attorney General enforcement mechanism.

(With concerns) We appreciate that you have worked very hard on this bill. We have seen a narrowing of the focus on this bill to RFID devices. However, we are concerned that this language may still include some wireless devices. This bill, if it includes wireless devices, could have a devastating impact on our industry. We will lose customers if we give up their personal information. We support the responsible use of RFID technology.

(Opposed) High-tech crimes often require a high-tech solution. We already have sophisticated data protocols and don't feel that our customers' private information is at risk. This is a greatly improved bill. Compliance looks possible and it is much narrower. This does create some new business risks. We would prefer to see the Attorney General enforce the bill rather than a private right of action. We cannot support the bill as currently drafted because we feel it is aimed at the retail sector, but it also negatively impacts the health care sector. The health care industry is already highly regulated in terms of disclosure of personal information. We don't feel like an additional law is needed. Smart cards are much more secure than RFID tags. We feel this bill will stifle the use of beneficial technologies like RFID. Instead, it should crack down on nefarious use. We are opposed to the bill in the current draft because it encompasses access cards and proximity cards. They don't carry personal information on them. Labeling and deactivation for automobile application is difficult. Key fobs and tire pressure devices are implicated and it is problematic for us to have to label and possibly deactivate them.

Persons Testifying:

January 10, 2007
(In support) Representative Morris, prime sponsor; Leslie Simons Michelassi, Consumers Against Supermarket Privacy Invasion and Numbering; and Jeff Benton.

(In support with concerns) Jennifer Shaw, American Civil Liberties Union of Washington.

(With concerns) Dave Warren, Washington Public Utility Districts Association.

(Opposed) Russell Sarazen, T-Mobile; Steve Gano, Cingular Wireless; Denny Eliason, Washington Bankers Association; Lew McMurran, Washington Software Alliance; Mark

Johnson, Washington Retail Association; Allison Fleming, EPC Global; Caroline Silviera, Grocery Manufacturer's Association; and Nancy Atwood, American Electronics Association.

February 16, 2007
(In support) Representative Morris, prime sponsor; and Leslie Simons Michelassi, Consumers Against Supermarket Privacy Invasion and Numbering.

(In support with concerns) Teresa Atkinson, Washington State Coalition Against Domestic Violence; Jennifer Shaw, American Civil Liberties Union of Washington; Art Butler, WebTec.

(With concerns) Russell Sarazen, T-Mobile; Peter Their, Washington State Transit Association; and Candace Carlson, King County Metro Transit.

(Opposed) Joyce Masamitsu, Verizon Wireless; Dan Youmans, Cingular Wireless; Lew McMurran, Washington Software Alliance; Tom Byron, Washington State Hospital Association; Nancy Atwood, American Electronics Association; James Sheire, NXP Semiconductors; Mark Johnson, Washington Retail Association; Cliff Webster, HID Global, General Motors and PhRMA; and Nancee Wildermuth, Sprint Nextel, Regence Blue Shield and the Alliance of Auto Manufacturers.

Persons Signed In To Testify But Not Testifying: None.